

Advanced Web Search**Search with...**

this boolean
expression

("log table" OR "log tables") AND
(galois or rijndael) AND (256 OR
x256 OR times256)

**FIND**

Use terms such as AND, OR, NOT
[More>>](#)

SEARCH: ☐ Worldwide ☒ USA **RESULTS IN:** ☒ All languages ☐ [English, Spanish](#)

AltaVista found 140 results

Introduction to the new AES Standard: RijndaelFile type:PDF - [Download PDF Reader](#)

... **Rijndael** is a block cipher that encrypts and decrypts 128, 192, and 256 bit ... stands of Evariste **Galois**, who, before dying in ... of the **log table** is the logs ...

bass.gmu.edu/courses/ECE636/viewgraphs/rijndael_intro.PDF

[More pages from bass.gmu.edu](#)

www.cl.cam.ac.uk/Research/SRG/netos/xen/readmes/xeno-unstable.bk/ref-linux-2.4.30/drivers/char/ftape/lowlevel/ftape-ecc.c

/* * Copyright (c) 1993 Ning and David Mosberger. This is based on code originally written by Bas Laarhoven (bas@vimec.nl) and David L. Brown, Jr., and incorporates improvements suggested by Kai Harrekilde-Petersen.

www.cl.cam.ac.uk/Research/SRG/netos/xen/readmes/xeno-unstable...tape/lowlevel/ftape-ecc.c

[More pages from cl.cam.ac.uk](#)

www.cs.toronto.edu/~brewste/bkshelf/linux/src/V2.0.27a/linux/drivers/char/ftape/ecc.c

... the polynomials * in the **Galois** Field $GF(2^8)$. We ... 0xc3, 0x01 }; /* *

This is a **log table**. That is, gflog ... const unsigned char gflog[256] =

{ 0xff, 0x00, 0x01, 0x63, 0x02 ...

www.cs.toronto.edu/~brewste/bkshelf/linux/src/V2.0.27a/linux/drivers/char/ftape/ecc.c

[More pages from cs.toronto.edu](#)

ftape-ecc.c

File: /usr/src/linux-2.4.7/drivers/char/ftape/lowlevel/ftape-ecc.c

joshua.raleigh.nc.us/docs/linux-2.4.7_html/199285.html

[More pages from joshua.raleigh.nc.us](#)

Elliptic curve cryptography FAQ v1.12 22nd December 1997

Elliptic curve cryptography FAQ v1.12 22nd December 1997. by George Barwood. (1) What is an elliptic curve? Well for a start, it is not the same as an ellipse!

www.cryptoman.com/elliptic.htm

[More pages from cryptoman.com](#)

ietfreport.isoc.org/all-ids/draft-ietf-ipvbi-nabts-03.txt

IPVBI R. Panabaker, Microsoft Internet Draft S. Wegerif, Philips Semiconductors D. ... in the FEC **Galois** fields form the ... of the **Galois** field used in ... **Galois** Field is limited to 256 entries so the power and **log tables** are limited to 256 ...